To: **Illinois HIE Data Security & Privacy Committee**
From: **Infinite Systems Support**
Date: **July 17, 2012**
Re: **Patient Health Data Privacy & Security Policies**

Ira Thompson: Thank you very much; it is a pleasure to speak before this Committee.

The HIPAA Audit and Control Security Standard, 164.312, requires the covered entity to implement hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. The HIPAA standard also requires the covered entity have a mechanism for notifying and having detective controls in place such that if the protocol(s) or procedure(s) are breached a forensic review can be conducted to examine the activity.

All of these controls are in place within the HIE. Infinite Systems Support recommends a periodic review of HIE controls.

Ron Warren: Thank you for this opportunity.

It is our perspective that an audit framework should be standards-based and compliance-governed. It is one thing to have a standard that says 'this is what should be done' but without some type of governance structure to ensure there is compliance, there is no real reliability or credibility to the assessment. Infinite Systems Support has found that misuse of gatekeeper laws are generally more detective, after the fact, than preventative. A control framework must consist of both; the preventative controls that look at the design and then the operational controls to detect whether or not the system is operating as designed.

Our research also indicates that there are approaches to mental health data that put the patient's health first, addressing one of the concerns that we've seen in this area. We say our number one objective is the patient; it begs the question, what's more important, the patient's health or the patient's security of their information. Is it more important that patients are provided appropriate care based on knowing all the components of their conditions or is it more important that we protect their information so that the people who could use it to provider care do not even have access to it? Balancing these perspectives is a challenge everyone is facing.

Our perspective is that there is a lot of concern around the sensitivity of data sharing, and that is due to the lack of structure. Consumers are not comfortable that who they give their data to is going to use it responsibly and monitored to ensure compliance with applicable data sharing standards and policies. Not ensuring compliance with standards is like giving someone your check book and saying 'I trust that you won't write any checks, even though I don't have a signature identified'. No patient will maintain trust in the system without assurance that security standard compliance is enforced. It is the responsibility of the providers and of the State to ensure standards are in place and enforced.

Infinite Systems Support believes that a monitoring and compliance program is essential to ensuring the protection of patient information. And that the State has a fiduciary responsibility to ensure that happens for anyone that opts-in to the state HIE.

Finally, we talk a lot about patients and their access to data and whether they give consent. It is unclear what methodologies have been identified to give patients access to their data, for example a smart card

with their information; allowing patients to be in control of their potentially sensitive information, particularly as it relates to behavioral health.

We appreciate the opportunity to present before the group.